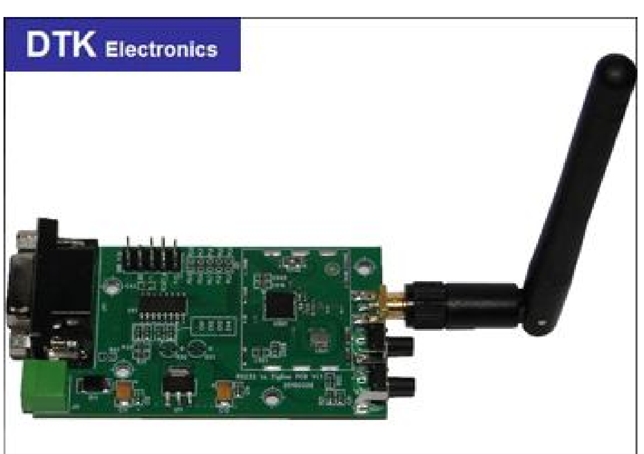


DTK 深圳市鼎泰克电子有限公司
SHENZHEN DIGITALTEK ELECTRONICS CO.,LTD

ZigBee 模块用户手册

V1.4





深圳市鼎泰克电子有限公司

地址：深圳市宝安区宝安大道卡罗大厦 2A 栋 505-506 室
电话：0755-29080800 29080900
E-Mail：yihua@sem.buaa.edu.cn
网址：www.dtkcn.com



目 录

一、ZigBee 概述（以下内容引自：百度百科，http://baike.baidu.com/view/117166.htm ）

什么是 ZigBee

ZigBee 是 IEEE 802.15.4 协议的代名词。根据这个协议规定的技术是一种短距离、低功耗的无线通信技术。这一名称来源于蜜蜂的八字舞，由于蜜蜂(bee)是靠飞翔和“嗡嗡”(zig)地抖动翅膀的“舞蹈”来与同伴传递花粉所在方位信息，也就是说蜜蜂依靠这样的方式构成了群体中的通信网络。其特点是近距离、低复杂度、自组织、低功耗、低数据速率、低成本。主要适合用于自动控制和远程控制领域，可以嵌入各种设备。

简而言之，ZigBee 就是一种便宜的，低功耗的近距离无线组网通讯技术。

ZigBee 的起源

ZigBee，在中国被译为"紫蜂",它与蓝牙相类似.是一种新兴的短距离无线技术．用于传感控制应用(sensor and control).此想法在 IEEE 802.15 工作组中提出,于是成立了 TG4 工作组,并制定规范 IEEE 802.15.4.



2002 年,ZigBee Alliance 成立.

2004 年,ZigBee V1.0 诞生.它是 ZigBee 的第一个规范.但由于推出仓促,存在一些错误.

2006 年,推出 ZigBee 2006,比较完善.

2007 年底,ZigBee PRO 推出



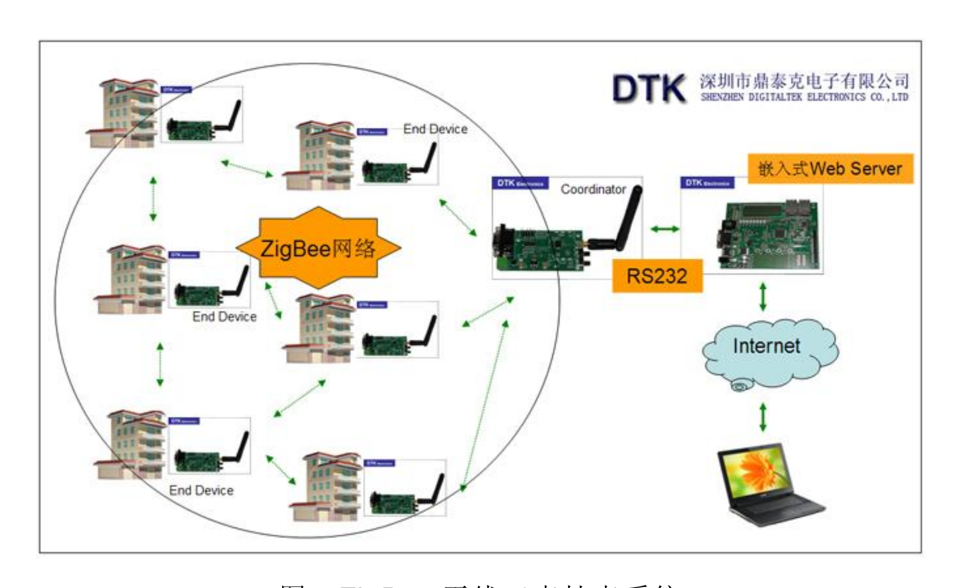
ZigBee 的底层技术基于 IEEE 802.15.4.

物理层和 MAC 层直接引用了 IEEE 802.15.4

在蓝牙技术的使用过程中，人们发现蓝牙技术尽管有许多优点，但仍存在许多缺陷。对工业，家庭自动化控制和工业遥测遥控领域而言，蓝牙技术显得太复杂，功耗大，距离近，组网规模太小等，而工业自动化，对无线数据通信的需求越来越强烈，而且，对于工业现场，这种无线数据传输必须是高可靠的，并能抵抗工业现场的各种电磁干扰。因此，经过人们长期努力，ZigBee 协议在 2003 年正式问世。另外，ZigBee 使用了在它之前所研究过的面向家庭网络的通信协议 Home RF Lite。

长期以来，低价、低传输率、短距离、低功率的无线通讯市场一直存在着。自从 Bluetooth 出现以后，曾让工业控制、家用自动控制、玩具制造商等业者雀跃不已，但是 Bluetooth 的售价一直居高不下，严重影响了这些厂商的使用意愿。如今，这些业者都参加了 IEEE802.15.4 小组，负责制定 ZigBee 的物理层和媒体介入控制层。IEEE802.15.4 规范是一种经济、高效、低数据速率（<250kbps）、工作在 2.4 GHz 和 868/928MHz 的无线技术，用于个人区域网和对等网络。它是 ZigBee 应用屋和网络层协议的基础。ZigBee 是一种新兴的近距离、低复杂度、低功耗、低数据速率、低成本的无线网络技术，它是一种介于无线标记技术和蓝牙之间的技术提案。主要用于近距离无线连接。它依据 802.15.4 标准，在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量，以接力的方式通过无线电波将数据从一个传感器传到另一个传感器，所以它们的通信效率非常高。

ZigBee 无线数据传输网络描述



图：ZigBee 无线三表抄表系统

简单的说，ZigBee 是一种高可靠的无线数传网络，类似于 CDMA 和 GSM 网络。ZigBee 数传模块类似于移动网络基站。通讯距离从标准的 75m 到几百米、几公里，并且支持无限扩展。

ZigBee 是一个由可多到 65000 个无线数传模块组成的一个无线数传网络平台，在整个网络范围内，每一个 ZigBee 网络数传模块之间可以相互通信，每个网络节点间的距离可以从标准的 75m 无限扩展。

与移动通信的 CDMA 网或 GSM 网不同的是，ZigBee 网络主要是为工业现场自动化控制数据传输而建立，因而，它必须具有简单，使用方便，工作可靠，价格低的特点。而移动通信网主要是为语音通

信而建立，每个基站价值一般都在百万元人民币以上，而每个 ZigBee“基站”却不到 1000 元人民币。每个 ZigBee 网络节点不仅本身可以作为监控对象，例如其所连接的传感器直接进行数据采集和监控，还可以自动中转别的网络节点传过来的数据资料。除此之外，每一个 ZigBee 网络节点(FFD)还可在自己信号覆盖的范围内，和多个不承担网络信息中转任务的孤立的子节点(RFD)无线连接。

ZigBee 采用的自组织网通信方式

ZigBee 技术所采用的自组织网是怎么回事？举一个简单的例子就可以说明这个问题，当一队伞兵空降后，每人持有一个 ZigBee 网络模块终端，降落到地面后，只要他们彼此间在网络模块的通信范围内，通过彼此自动寻找，很快就可以形成一个互联互通的 ZigBee 网络。而且，由于人员的移动，彼此间的联络还会发生变化。因而，模块还可以通过重新寻找通信对象，确定彼此间的联络，对原有网络进行刷新。这就是自组织网。

ZigBee 技术为什么要使用自组织网来通信？

网状网通信实际上就是多通道通信，在实际工业现场，由于各种原因，往往并不能保证每一个无线通道都能够始终畅通，就像城市的街道一样，可能因为车祸，道路维修等，使得某条道路的交通出现暂时中断，此时由于我们有多个通道，车辆（相当于我们的控制数据）仍然可以通过其他道路到达目的地。而这一点对工业现场控制而言则非常重要。

为什么自组织网要采用动态路由的方式？

所谓动态路由是指网络中数据传输的路径并不是预先设定的，而是传输数据前，通过对网络当时可利用的所有路径进行搜索，分析它们的位置关系以及远近，然后选择其中的一条路径进行数据传输。在我们的网络管理软件中，路径的选择使用的是“梯度法”即先选择路径最近的一条通道进行传输，如传不通，再使用另外一条稍远一点的通路进行传输，以此类推，直到数据送达目的地为止。在实际工业现场，预先确定的传输路径随时都可能发生变化，或者因各种原因路径被中断了，或者过于繁忙不能进行及时传送。动态路由结合网状拓扑结构，就可以很好解决这个问题，从而保证数据的可靠传输。

ZigBee 自身的技术优势

①低功耗。在低耗电待机模式下,2 节 5 号干电池可支持 1 个节点工作 6～24 个月,甚至更长。这是 ZigBee 的突出优势。相比较，蓝牙能工作数周、WiFi 可工作数小时。

现在，TI 公司和德国的 Micropelt 公司共同推出新能源的 ZigBee 节点。该节点采用 Micropelt 公司的热电发电机给 TI 公司的 ZigBee 提供电源。

②低成本。通过大幅简化协议(不到蓝牙的 1/10) ,降低了对通信控制器的要求,按预测分析,以 8051 的 8 位微控制器测算,全功能的主节点需要 32KB 代码,子功能节点少至 4KB 代码,而且 ZigBee 免协议专利费。每块芯片的价格大约为 2 美元。

③ 低速率。ZigBee 工作在 20～250 kbps 的较低速率,分别提供 250 kbps(2.4GHz)、40kbps (915 MHz)和 20kbps(868 MHz) 的原始数据吞吐率,满足低速率传输数据的应用需求。

④近距离。传输范围一般介于 10～100 m 之间,在增加 RF 发射功率后,亦可增加到 1～3 km。这指的是相邻节点间的距离。如果通过路由和节点间通信的接力,传输距离将可以更远。

⑤短时延。ZigBee 的响应速度较快,一般从睡眠转入工作状态只需 15 ms ,节点连接进入网络只需 30 ms ,进一步节省了电能。相比较,蓝牙需要 3～10 s、WiFi 需要 3 s。

⑥高容量。ZigBee 可采用星状、片状和网状网络结构,由一个主节点管理若干子节点,最多一个主节点可管理 254 个子节点;同时主节点还可由上一层网络节点管理,最多可组成 65000 个节点的大网。

⑦高安全。ZigBee 提供了三级安全模式,包括无安全设定、使用接入控制清单(ACL) 防止非法获取数据以及采用高级加密标准(AES 128) 的对称密码,以灵活确定其安全属性。

⑧免执照频段。采用直接序列扩频在工业科学医疗(ISM) 频段,2. 4 GHz (全球) 、915 MHz(美国) 和 868 MHz(欧洲) 。

ZigBee 的频带

1) 868MHZ 传输速率为 20KB/S 适用于欧洲

2) 915MHZ 传输速率为 40KB/S 适用于美国

3) 2.4GHZ 传输速率为 250KB/S 全球通用

由于 此三个频带物理层并不相同,其各自信道带宽也不同,分别为

0.6MHZ,2MHZ 和 5MHZ.分别有 1 个 10 个和 16 个信道.

不同频带的扩频和调制方式有区别.虽然都使用了直接扩频(DSSS)的方式,但从比特到码片的变换方式有较大的差别.

调制方式都用了调相技术,但 868MHZ 和 915MHZ 频段采用的是 BPSK

而 2.4GHZ 频段采用的是 OQPSK

在发射功率为 0dBm 的情况下,BLUETOOTH 通常能用 10M 的作用范围.

而基于 IEEE 802.15.4 的 ZigBee 在室内通常能达到 30-50 米作用距离,在室外如果障碍物少,甚至可以达到 100 米作用距离.

所以 ZigBee 可归为低速率的短距离无线通信技术.

ZigBee 性能分析

1，数据速率比较低 在 2.4GHZ 的频段只有 250Kb/S,而且只是链路上的速率,除掉信道竞争应答和重传等消耗,真正能被应用所利用的速率可能不足 100Kb/S,并且余下的速率可能要被邻近多个节点和同一个节点的多个应用所瓜分.因此不适合做视频之类事情.

适合的应用领域--------传感和控制

2，可靠性 在可靠性方面,ZigBee 有很多方面进行保证.物理层采用了扩频技术,能够在一定程度上抵抗干扰

MAC 应用层(APS 部分)有应答重传功能.

MAC 层的 CSMA 机制使节点发送前先监听信道,可以起到避开干扰的作用.

当 ZigBee 网络受到外界干扰,无法正常工作时,整个网络可以动态的切换到另一个工作信道上.

3，时延 由于 ZigBee 采用随机接入 MAC 层,且不支持时分复用的信道接入方式,因此不能很好的支持一些实时的业务.

4，能耗特性 能耗特性是 ZigBee 的一个技术优势.

通常 ZigBee 节点所承载的应用数据速率都比较低,在不需要通信时,节点可以进入很低功耗的休眠状态,此时能耗可能只有正常工作状态下的千分之一.由于一般情况下,休眠时间占总运行时间的大部分,有时正常工作的时间还不到百分之一,因此达到很高的节能效果.

5，组网和路由性------网络层特性

ZigBee 大规模的组网能力--------每个网络 65000 个节点

Bluetooth-------每个网络 8 个节点.

因为 ZigBee 底层采用了直扩技术,如果采用非信标模式,网络可以扩展得很大,因为不需同步而且节点加入网络和重新加入网络的过程很快,一般可以做到 1 秒以内,甚至更快.

Bluetooth 通常需要 3 秒

在路由方面,ZigBee 支持可靠性很高的网状网的路由,所以可以布置范围很广的网络,并支持多播和广播特性,能够给丰富的应用带来有力的支持.

ZigBee 的应用前景

ZigBee 并不是用来与蓝牙或者其他已经存在的标准竞争，它的目标定位于现存的系统还不能满足其需求的特定的市场，它有着广阔的应用前景。ZigBee 联盟预言在未来的四到五年，每个家庭将拥有 50 个 ZigBee 器件，最后将达到每个家庭 150 个。据估计，到 2007 年，ZigBee 市场价值将达到数亿美元。其应用领域主要包括：

◆家庭和楼宇网络：空调系统的温度控制、照明的自动控制、窗帘的自动控制、煤气计量控制、家用电器的远程控制等；

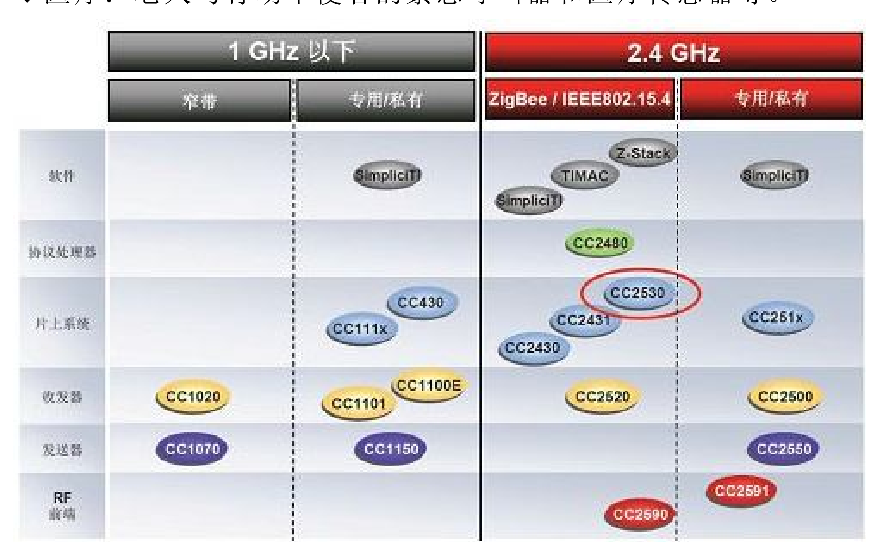
◆工业控制：各种监控器、传感器的自动化控制；

◆商业：智慧型标签等；

◆公共场所：烟雾探测器等；

◆农业控制：收集各种土壤信息和气候信息；

◆医疗：老人与行动不便者的紧急呼叫器和医疗传感器等。



图：TI RF 产品 Road Map

ZigBee 联盟

ZigBee 联盟是一个高速成长的非盈利业界组织，成员包括国际著名半导体生产商、技术提供者、技术集成商以及最终使用者。联盟制定了基于 IEEE802.15.4，具有高可靠、高性价比、低功耗的网络

应用规格。

ZigBee 联盟的主要目标是以通过加入无线网络功能，为消费者提供更富有弹性、更容易使用的电子产品。ZigBee 技术能融入各类电子产品，应用范围横跨全球的民用、商用、公共事业以及工业等市场。使得联盟会员可以利用 ZigBee 这个标准化无线网络平台，设计出简单、可靠、便宜又节省电力的各种产品来。

ZigBee 联盟所锁定的焦点为制定网络、安全和应用软件层；提供不同产品的协调性及互通性测试规格；在世界各地推广 ZigBee 品牌并争取市场的关注；管理技术的发展。

ZigBee 联盟对 ZigBee 标准的制定：IEEE802.15.4 的物理层、MAC 层及数据链路层，标准已在 2003 年 5 月发布。ZigBee 网络层、加密层及应用描述层的制定也取得了较大的进展。V1.0 版本已经发布。其他应用领域及其相关的设备描述也会陆续发布。由于 ZigBee 不仅只是 802.15.4 的代名词，而且 IEEE 仅处理低级 MAC 层和物理层协议，因此 ZigBee 联盟对其网络层协议和 API 进行了标准化。完全协议用于一次可直接连接到一个设备的基本节点的 4K 字节或者作为 Hub 或路由器的协调器的 32K 字节。每个协调器可连接多达 255 个节点，而几个协调器则可形成一个网络，对路由传输的数目则没有限制。ZigBee 联盟还开发了安全层，以保证这种便携设备不会意外泄漏其标识，而且这种利用网络的远距离传输不会被其它节点获得。

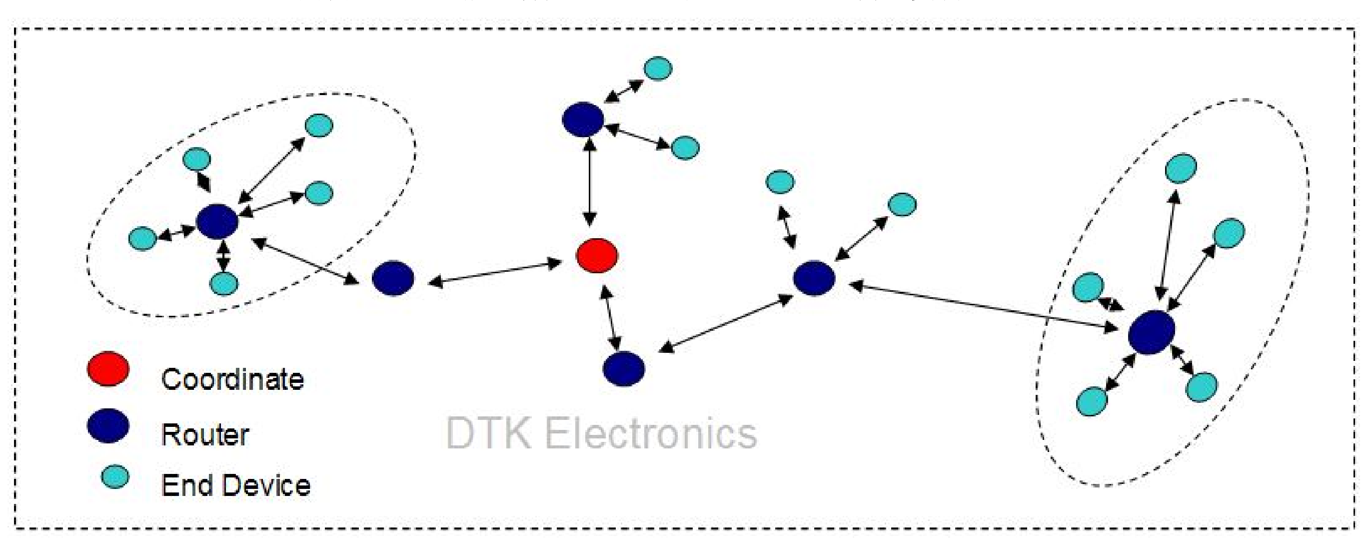
ZigBee 的网络拓扑

在 ZigBee 网络中，定义了三种网络角色，分别是 Coordinator（网络协调器节点），Router（网络路由器节点），End Device（网络终端节点）。

Coordinator（网络协调器节点）：负责网络的建立（WPAN Formation）及网络地址（Short Address）的分配；

Router（网络路由器节点）：负责找寻、建立及修复资料包路由路径（Routing Path），并负责转送资料包，同时也可配置网络地址（Short Address）给子节点（Child）；

End Device（网络终端节点）：只能选择加入已经形成的网络，可传送资料；





二、DRF 系列 ZigBee 模块特点

DRF 系列 ZigBee 模块目前包括 DRF1601,DRF1602,它是基于 TI 公司 CC2530F256 芯片,运行 ZigBee2007/PRO 协议的 ZigBee 模块，它具有 ZigBee 协议的全部特点，这有区别于其它种类的 ZigBee 模块（可能不是运行 Full ZigBee2007 协议，因为 ZigBee2007 协议的运行需要 256K 的 FLASH 空间）。

自动组网，上电即用是 DRF 系列 ZigBee 模块的主要特点。针对目前产品开发进度要求紧，市场变化快的特点，DTK 推出了自动组网，上电即用的 ZigBee 模块，用户不需要了解复杂的 ZigBee 协议，所有的 ZigBee 协议的处理部分，在 ZigBee 模块内部自动完成，用户只需要通过串口传输数据即可，是目前市场上应用 ZigBee 最简单的方式。

其主要特点包括：

DRF1600 系列 ZigBee 模块可以形象的理解为“无线的 RS232 连接”，所以使用这个模块就像使用 RS232 电缆一样简单。

- **自动组网：**所有的模块上电即自动组网，Coordinator 自动给所有的节点分配地址，不需要用户手动分配地址，网络加入应答等专业 ZigBee 组网流程；
- **简单数据传输：**通过串口即可在任意节点间进行数据传播（Router 只进行数据转发，不接收/输出串口数据），数据传输的格式为：0xFD（数据传输命令）＋0x0A（数据长度） ＋0x73 0x79（目标地址） ＋0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10（数据，共 0x0A Bytes）；
- **简单易用：**不用考虑 ZigBee 协议，自动组网；
- **高安全性：**无线数据空中加密；
- **唯一 IEEE 地址：**DRF 系列模块采用的 TI CC2530F256 芯片，出厂时已经自带 IEEE 地址，用户无需另行购买 IEEE 地址；

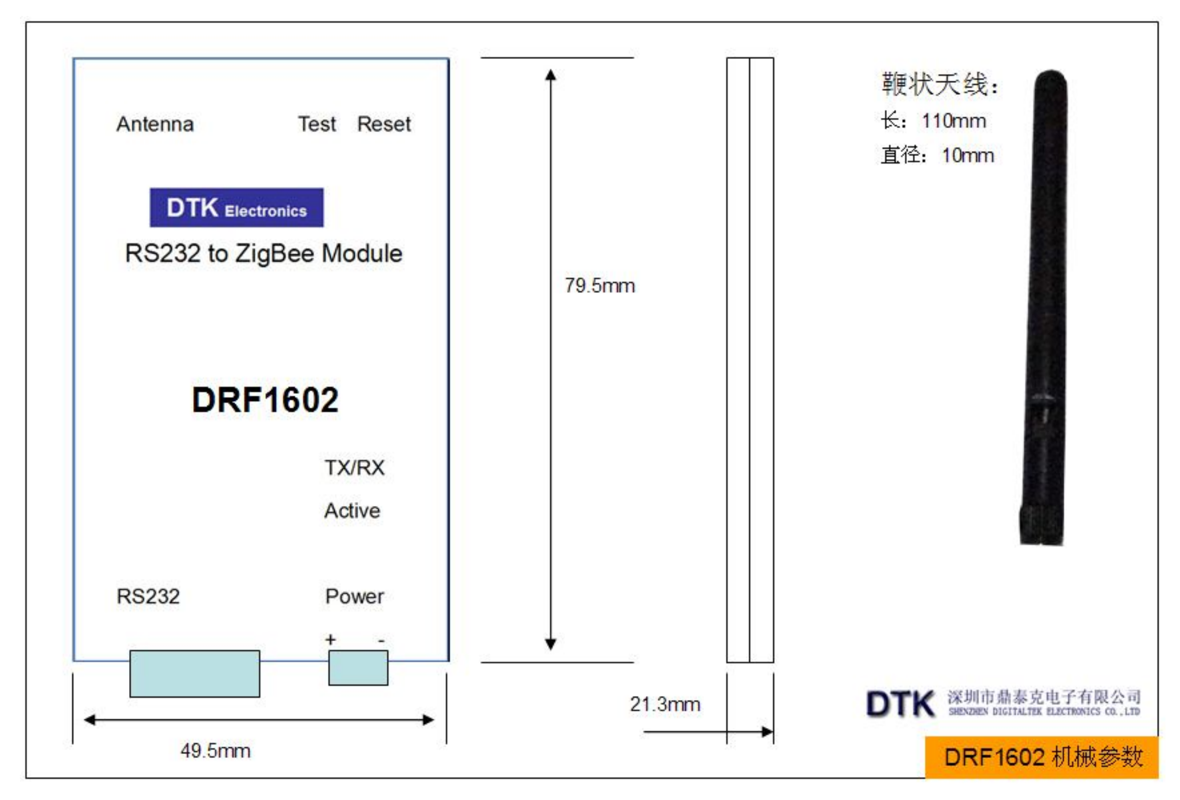


三、DRF 系列 ZigBee 模块参数

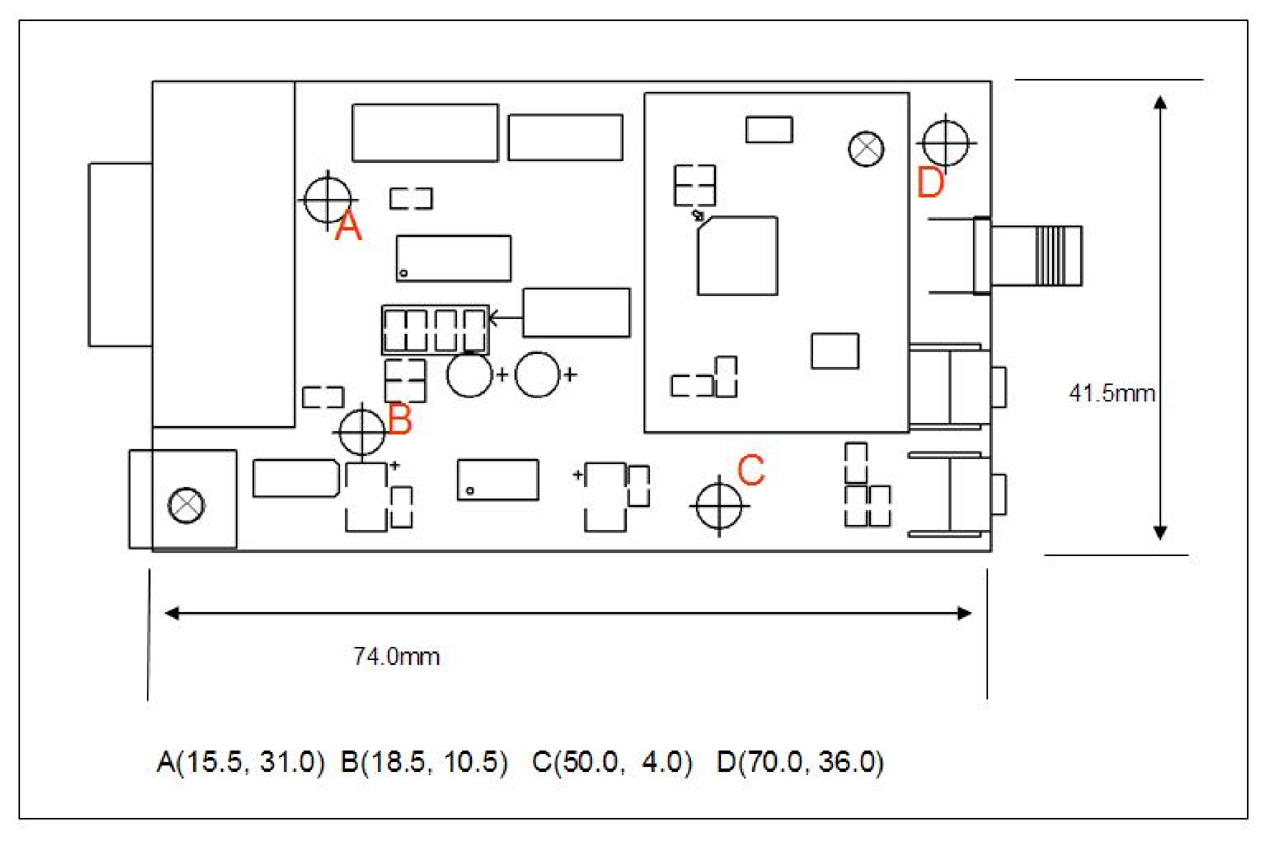
1，电气参数

输入电压：DC 5-9V
温度范围：-40⁰C --85⁰C
串口速率：38400bps（默认），可选 9600bps, 19200bps, 38400bps, 115200bps。
无线频率：2.4GHz
无线协议：ZigBee2007 /PRO
传输距离：可视距离 400 米
发射电流：34mA（最大）
接收电流：25mA（最大）
低功耗模式：可设定进入低功耗模式（与应用模式相关），2 节 AA 电池可使用半年
接收灵敏度：-96DBm
主芯片：CC2530F256，256KFLASH，TI 公司最新一代 ZigBee SOC 芯片

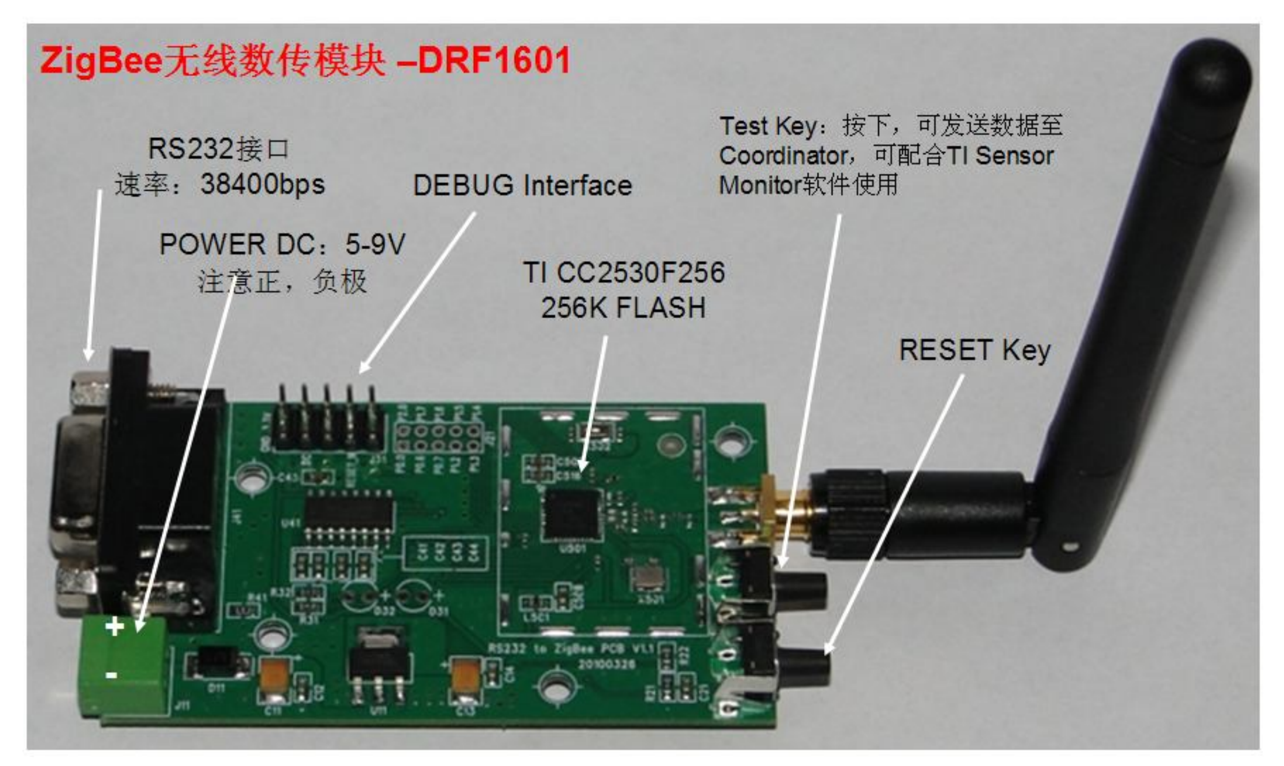
2，机械参数



DRF1602 主要尺寸：79.5 * 49.5 * 21.3mm



DRF1601 主要尺寸： 74 * 41.5 mm



DRF1601 内部结构



四、DRF 系列 ZigBee 模块的组网

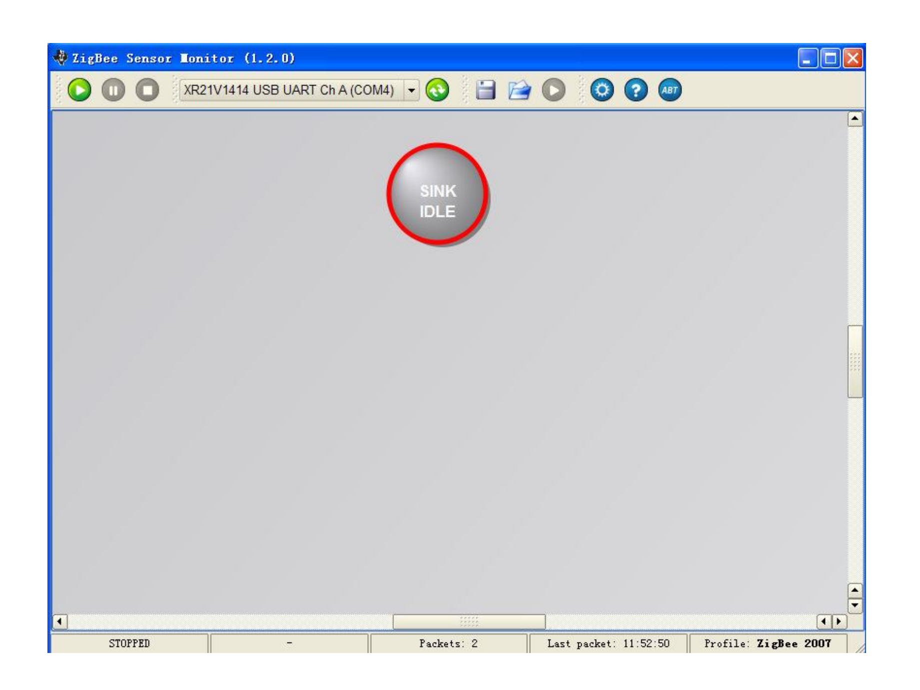
构成 ZigBee 网络的要素：

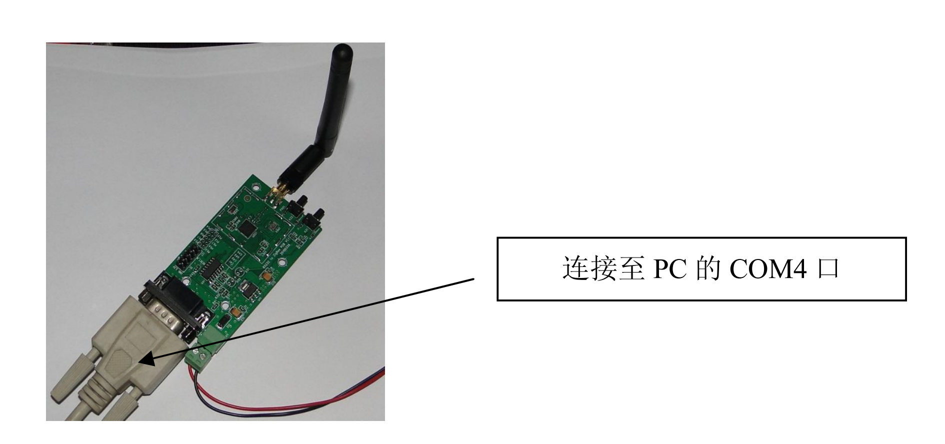
1，各节点使用相同的频率（出厂已设定）。

2，各节点使用同一 PAN ID（出厂已设定为 0x199B），如果要在相邻的空间组成不同的 ZigBee 网络，可以设定二组节点的 PAN ID 不同（通过串口设定）。

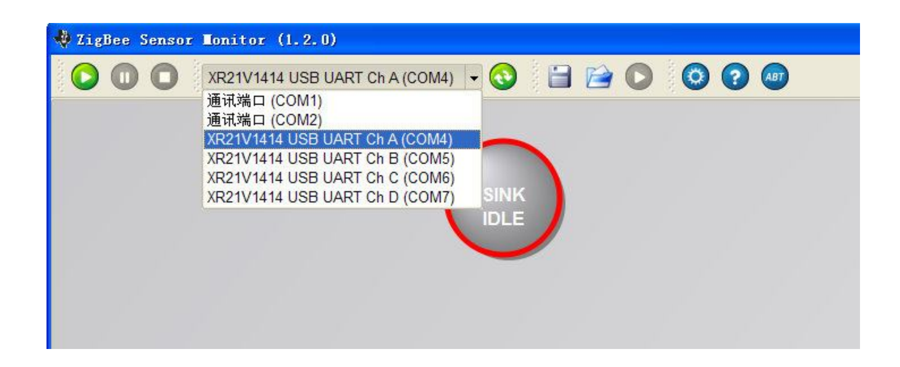
为了可视 ZigBee 模块的组网过程，DRF1601/1602 设定兼容 TI 的 Sensor Monitor 软件，可以通过 TI 的 Sensor Monitor 软件来监控组网过程，用户可在 TI 网站下载该软件：http://www.ti.com/cn/litv/zip/swrc096d

1，打开 TI Sensor Monitor 软件，将 Coordinator 模块通过串口连接至 PC。

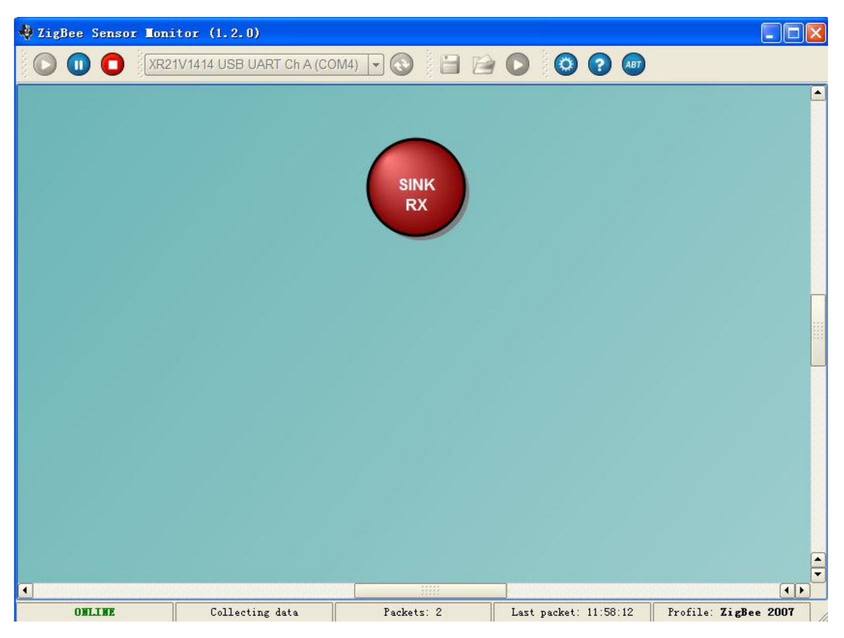




2，选取 Coordinator 连接的串口号，并点击 RUN 图标，运行

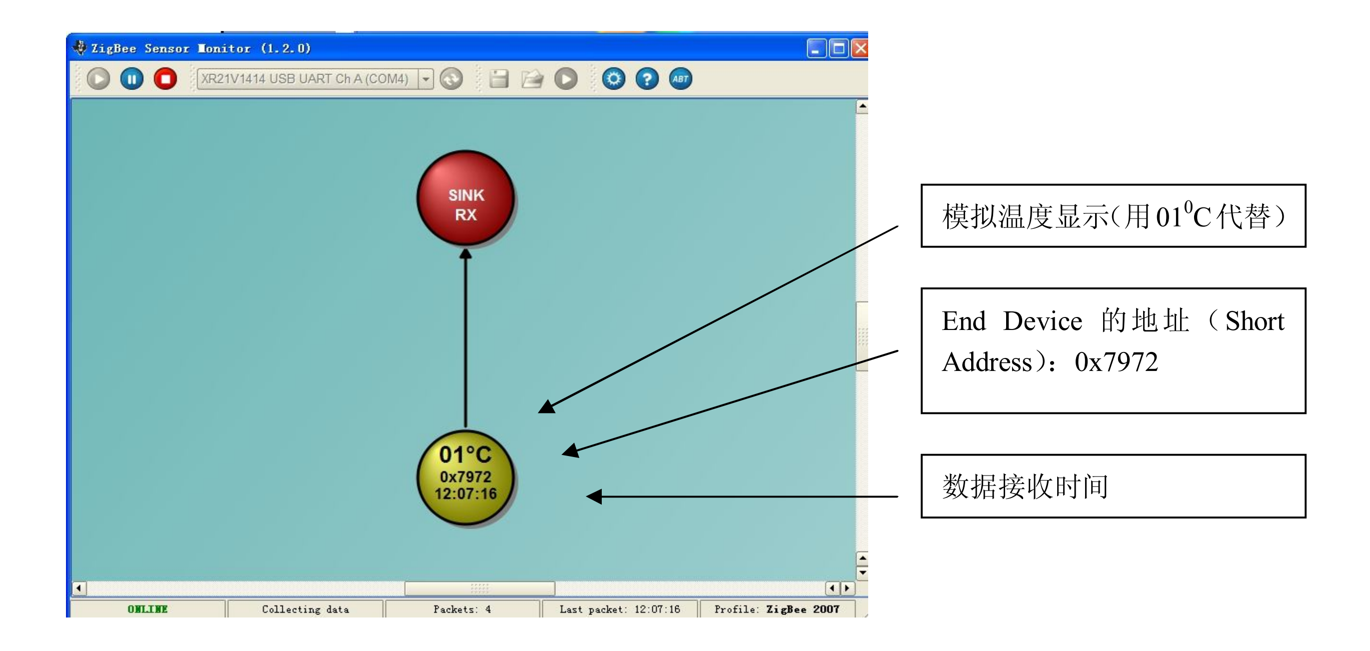


3，此时可以看到表示 Coordinator 的图标变成红色，表示 Coordinator 与 PC 连接成功：

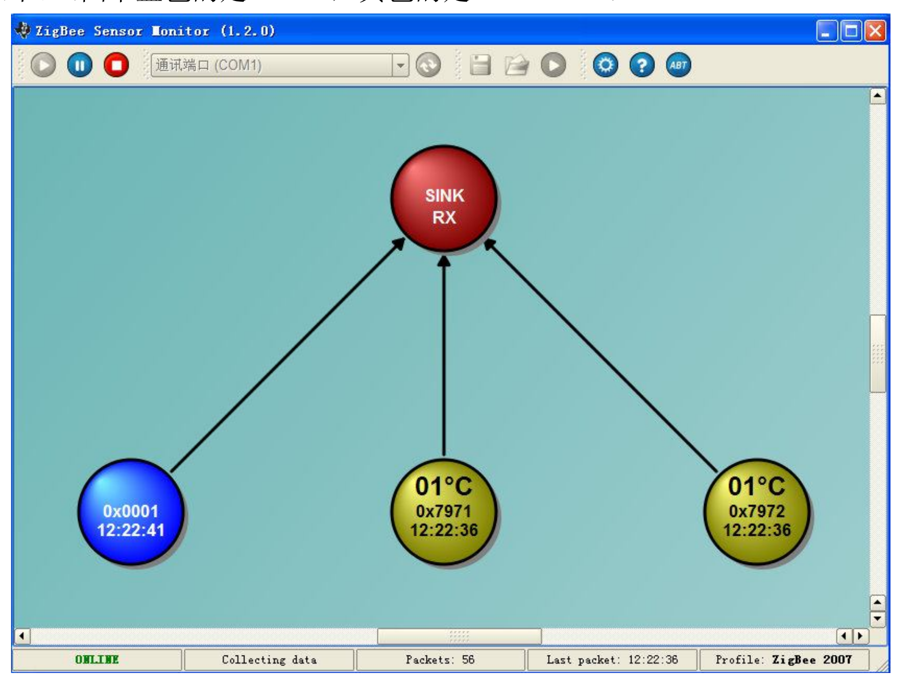


4，将一个 End Device 模块上电，并按一下 TEST 按钮，此时，End Device 模块会发送一个模拟数据到 Coordinator，Coordinator 会把这个数据通过串口发送到 PC（上面的实例是 COM4），并在 TI Sensor Monitor 软件里显示出网络结构，如下图：

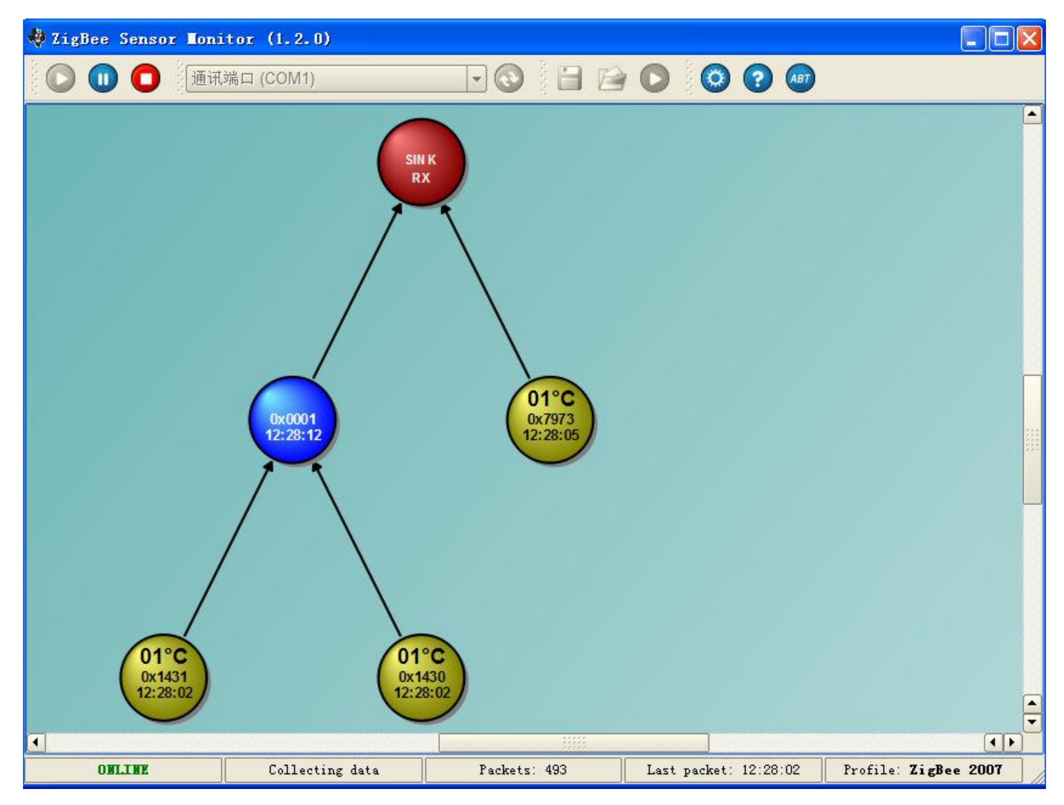
地址：深圳市宝安区宝安大道卡罗大厦 2A 栋 505-506 室　网址：www.dtkcn.com



5，同理，将其它的 End Device 模块或 Router 模块上电，则它们会自动寻找并加入这个网络，组网后的结构如下：（图中蓝色的是 Router，黄色的是 End Device）



或者，它是一个通过 Router 转发的网络：

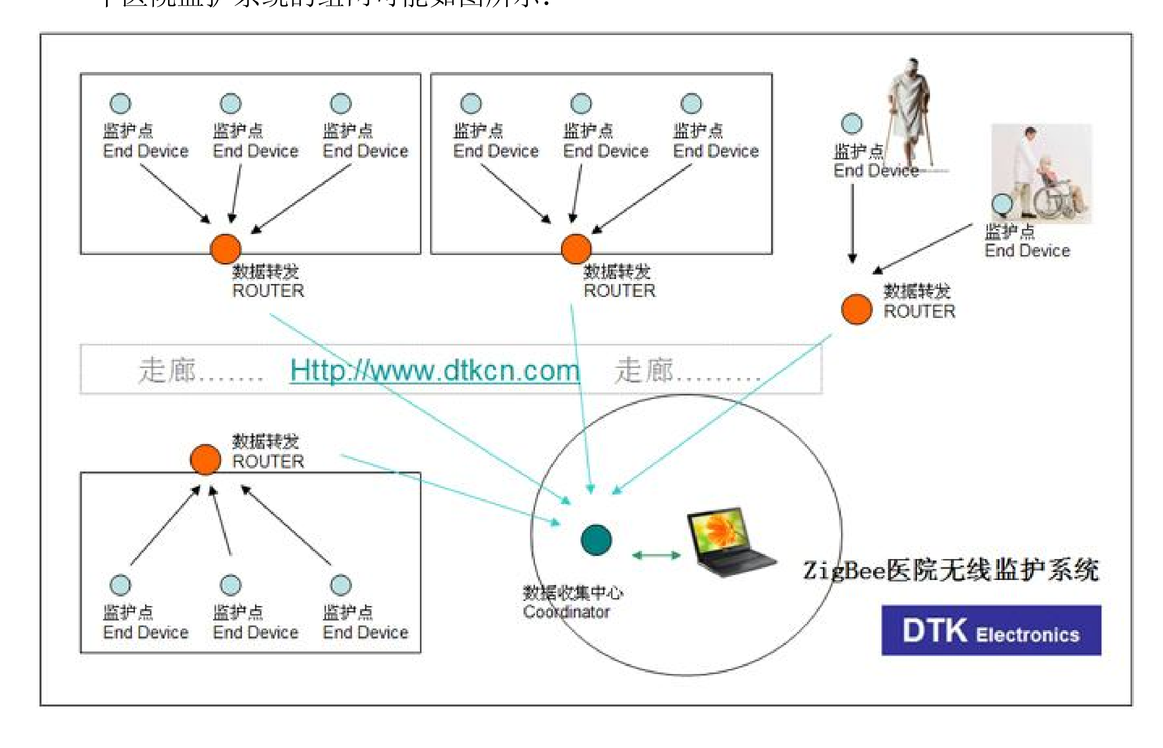


三个 End Device 的地址分别是：0x7973, 0x1430，0x1431
Router 的地址是：0x0001
Coordinator 的地址是：0x0000（Coordinator 永远是这个地址）

在上面的二张图片中可以发现，End Device 的地址会发生改变的，在此实例中，当二个 End Device 直接连接到 Coordinator 时，它的 Address 是 0x7971,0x7972，而当它通过 Router 转发时，Address 变成了 0x1430,0x1431。

组网实例：

一个医院监护系统的组网可能如图所示：





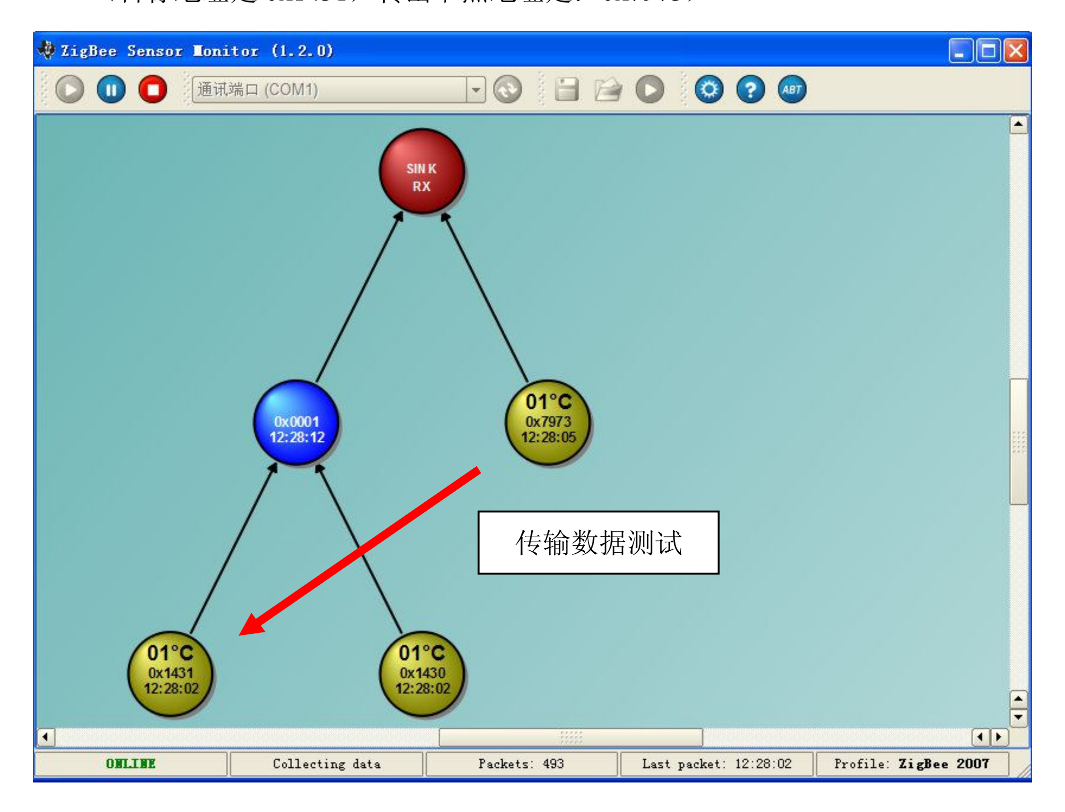
五、DRF 系列 ZigBee 模块的数据传输

DRF1601/1602 的数据传输功能非常易用，一条数据传输的命令格式如下：

数据传送指令(0xFD) ＋ 数据长度 ＋ 目标地址 ＋ 数据(默认最多 32Bytes,可根据应用调整最大 256Bytes)

如，我们来传送如下的数据：

（目标地址是 0x1431，传出节点地址是：0x7973）



数据格式如下：

0xFD 0x0A 0x31 0x14 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10

0xFD：数据传送指令

0x0A：数据长度（数据区的数据长度）

0x31 0x14：目标地址，低位在前，合起来是 0x1431

0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10：传送的数据

用串口调试程序来测试：

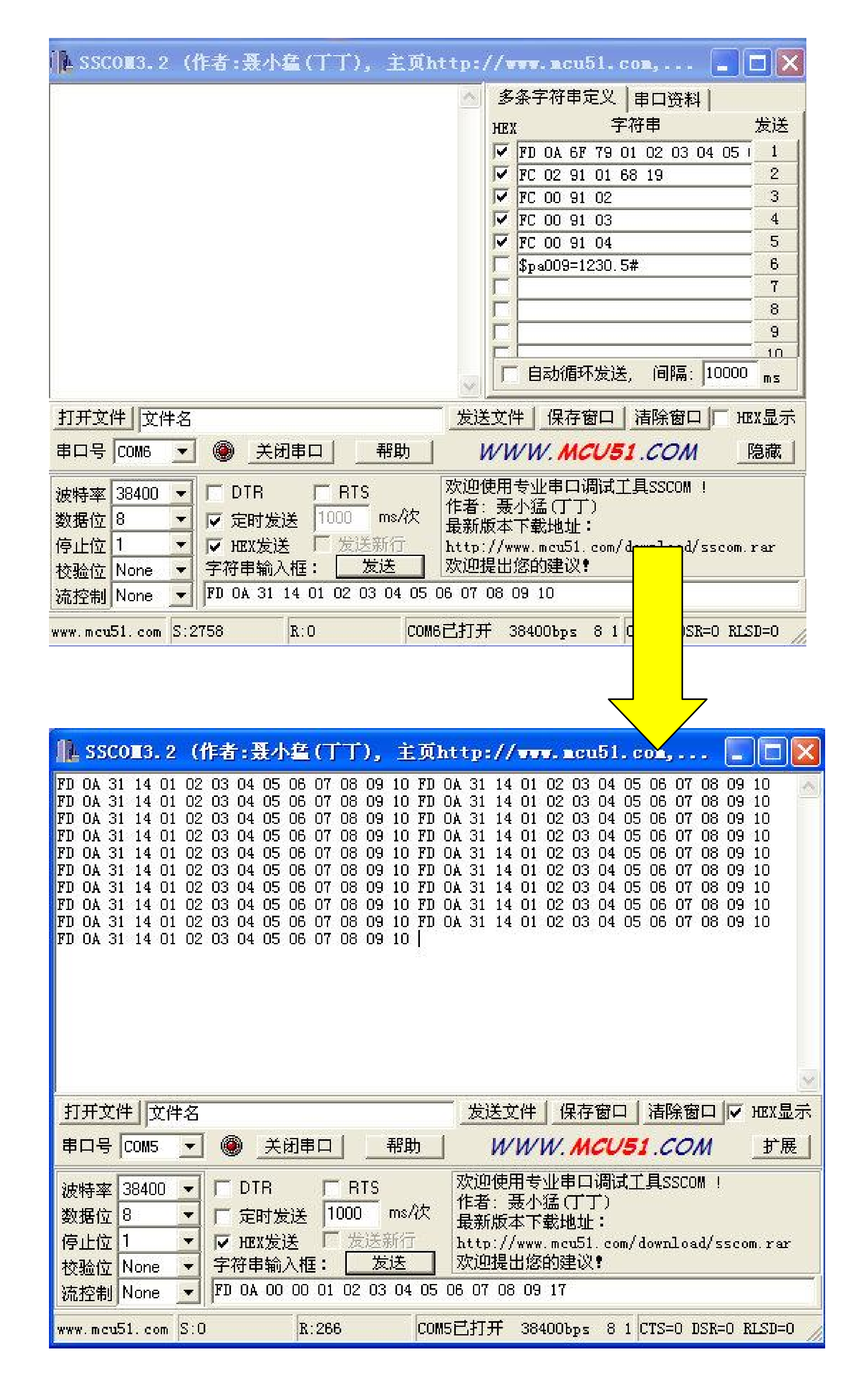
（0x7973 连接至：COM6，0x1431 连接至 COM5）

0x7973 传送的数据为：0xFD 0x0A 0x31 0x14 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10

0x1431 接收到的数据为：0xFD 0x0A 0x31 0x14 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x10

如下图所示：

地址：深圳市宝安区宝安大道卡罗大厦 2A 栋 505-506 室　　网址：www.dtkcn.com



同理，可在其它节点之间传送数据。格式如下：

1， 如果数据在 End Device 之间传送，则发送数据=接收数据；

2， 如果数据是 Coordinator 发送至 End Device，则发送数据=接收数据；

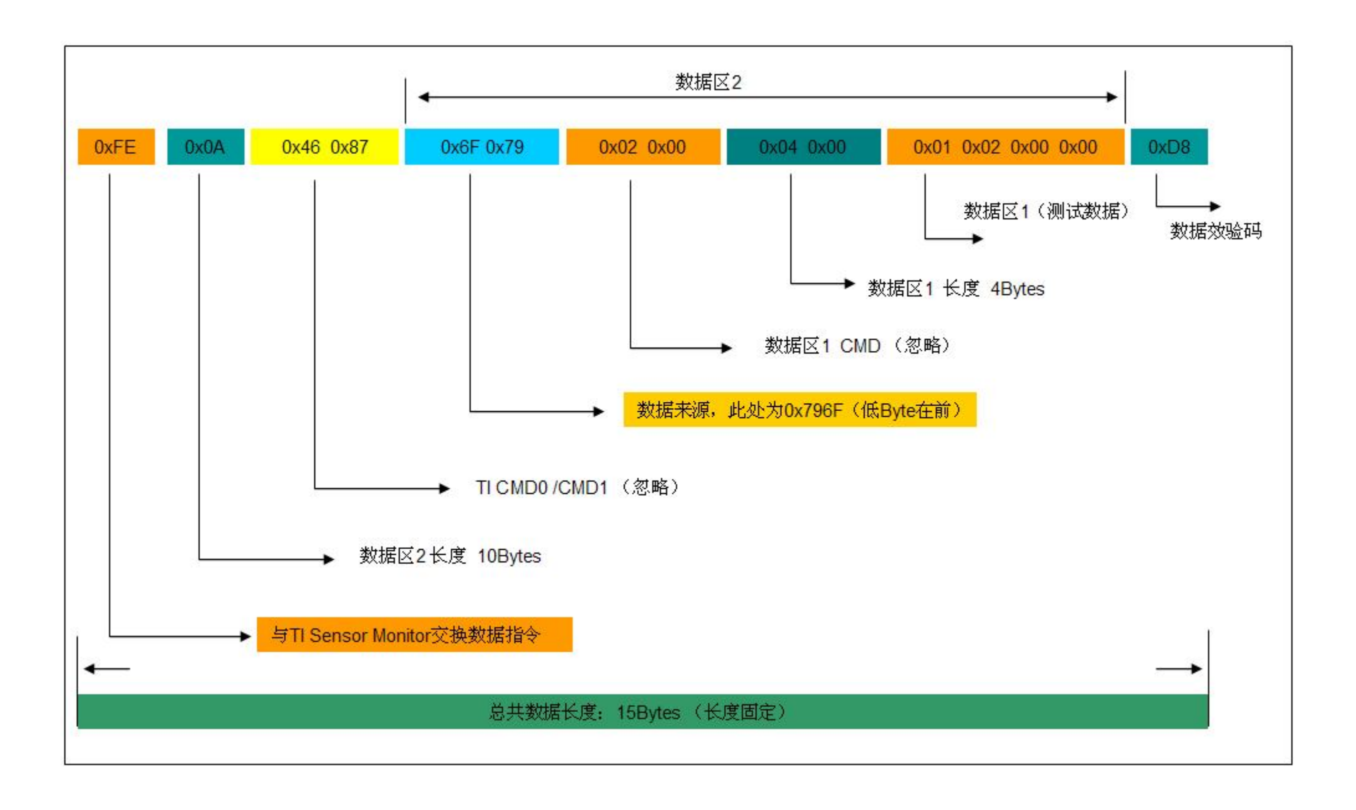
3， 如果数据是 End Device 发送给 Coordinator，则接收数据=TI Sensor Monitor 数据 + 发送数据。具体如下：



一个 End Device 的发送数据为：
0xFD 0x0A 0x00 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x15

则，Coordinator 接收并发送给 PC 的数据为：
0xFE 0x0A 0x46 0x87 0x6F 0x79 0x02 0x00 0x04 0x00 0x01 0x02 0x00 0x00 0xD8 0xFD 0x0A 0x00 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x15

这个数据分二部分：0xFE 开头的 15Bytes，用来提供给 TI Sensor Monitor，观察网络结构
0xFD 开头的部分，是接收到的数据，接收数据=发送数据（来自 End Device）
详解：
0xFE 0x0A 0x46 0x87 0x6F 0x79 0x02 0x00 0x04 0x00 0x01 0x02 0x00 0x00 0xD8



0xFD 0x0A 0x00 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x15
从 End Device 接收到的数据
0xFD：数据交换指令
0x0A：数据长度（不包含指令与目标地址）
0x00 0x00：目标地址（0x0000 是 Coordinator 地址）
0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x15：接收到的数据

4，Router 只承担数据的转发，网络中继任务，串口不接收及发送数据



六、DRF 系列 ZigBee 模块的设置

（1），设置模块的 PAN ID 为特定数值（如：0x1968）

0xFC 数据长度（1 Bytes） 命令格式（91 01 ：写入 PAN ID） PAN ID 数值（低位在前）

FC 02 91 01 68 19

（必须重新启动才生效，可按 RESET 健）

（2），设置模块的 PAN ID 为默认值（0x199B）

0xFC 数据长度（1 Bytes） 命令格式（91 02 ：写入 PAN ID）

FC 00 91 02

（必须重新启动才生效，可按 RESET 健）

（3），读取模块的 PAN ID

0xFC 数据长度（1 Bytes） 命令格式（91 03 ：读取 PAN ID）

FC 00 91 03

返回：9B 19 （模块的 PAN ID 为 0x199B）

（4），读取模块的地址（Short Address）

0xFC 数据长度（1 Bytes） 命令格式（91 04 ：读取 Short Address）

FC 00 91 04

返回：6F 79 （模块的 Short Address 为 0x796F）

（5），设置串口波特率：

默认的波特率是：38400bps，更改波特率没有开放，客户可选 9600,19200,38400,115200。